Final Examination
Coding Theory

23^{rd} February 2006

Time: 3 hours (12:30–3:30pm)

1. A channel matrix P is a matrix whose elements p_{ij} has the value of the probability that an input a_i in an input alphabet Σ_1 will produce an output b_j in an output alphabet Σ_2. The r^{th} *extension* of this channel is the discrete memoryless channel with input alphabet $\Sigma_1^{(r)} = a_1 a_2 \dots a_r$, output alphabet $\Sigma_2^{(r)} = b_1 b_2 \dots b_r$, and channel matrix $P^{(r)}$ whose components are $p_{ij}^{(r)} = p(b_1|a_1)\, p(b_2|a_2) \cdots p(b_r|a_r)$. Furthermore, P is said to be a *stochastic matrix* if $p_{ij} \geq 0$ for all i, j and all row sums are equal to 1, that is to say,

$$\sum_j p_{ij} = 1$$

a. Consider a binary symmetric channel, that is to say, a mapping from input to output such that $\Sigma_1 = \Sigma_2 = \{0, 1\}$. The second extension of this channel has input and output alphabet $\{00, 01, 10, 11\}$. If the channel matrix for this binary channel is

$$p = \begin{bmatrix} q & p \\ p & q \end{bmatrix}$$

what would be the channel matrix for the second extension of this channel? [4] Find $P^{(2)}$, if it is stochastic. [2]

b. Next, consider the binary erasure channel whose input alphabet is $\Sigma_1 = \{0, 1\}$ and output alphabet $\Sigma_2 = \{0, 1, *\}$. The channel matrix in this case may be described as

$$P = \begin{bmatrix} 1-\varepsilon & 0 & \varepsilon \\ 0 & 1-\varepsilon & \varepsilon \end{bmatrix}$$

Find the channel matrix for the second extension of this channel. [9]

2.

a. Explain *uncertainty* and *entropy*, *conditional entropy*, and *mutual information*, giving examples where appropriate. [2]

b. Let $H(X)$ be the entropy of a random variable X that takes on a finite set of values with probabilities $p_1, p_2, \dots, p_n$, that is $H(X) = -\sum_k p_k \ln p_k$. Show how the following statements are true. [8]

i. $H(p_1, \dots, p_n)$ is at maximum when $p_1 = p_2 = \dots = p_n = \frac{1}{n}$

ii. $H(p_1, \dots, p_n) = H\left(p_{\pi(1)}, \dots, p_{\pi(n)}\right)$

iii. $H(p_1, \dots, p_n) \geq 0$, where the equality holds only when one of the p_i's is 1.

iv. $H(p_1, \dots, p_n, 0) = H(p_1, \dots, p_n)$

v.
$$H\left(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n}\right) \leq H\left(\frac{1}{n+1}, \frac{1}{n+1}, \dots, \frac{1}{n+1}\right)$$

vi. $H(p_1, \dots, p_n)$ is a continuous function of its arguments.

vii.
$$H\left(\frac{1}{mn}, \frac{1}{mn}, \dots, \frac{1}{mn}\right) = H\left(\frac{1}{m}, \dots, \frac{1}{m}\right) + H\left(\frac{1}{n}, \dots, \frac{1}{n}\right)$$

viii. Let $p = p_1 + \cdots + p_m$ and $q = q_1 + \cdots + q_n$, where $p + q = 1$, p and q are positive and p_i and p_j non-negative. Then,

$$H(p_1, \dots, p_m, q_1, \dots, q_n) = H(p, q) + pH(p, q) + pH\left(\frac{p_1}{p}, \dots, \frac{p_m}{p}\right) + qH\left(\frac{q_1}{q}, \dots, \frac{q_n}{q}\right)$$

3.

a. Give the meaning and explanation of the terms *cryptography*, *cryptanalysis*, *cryptology*, *key*, *plain text*, *code*, *cipher*, *encode*, *decode*, *encrypt*, *decrypt* and *nondeterministic polynomial–complete*. [6]
b. Caesar cipher shifts all message letters three positions to the right on the ordered list of characters of the roman alphabet. Encode the previous sentence using Caesar cipher. [3]
c. One of the most basic encryption algorithms is the transposition of order d, in which the message is divided into blocks of length d and then a permutation π of $1, 2, \ldots, d$ is applied to each block. As an example, when $d = 5$ and $\pi = \{3\,4\,5\,2\,1\}$, Shakespeare's 'Fair is foul, and foul is fair' is encrypted into 'rfai fis a ul,siul ri fa'. Again, let $d = 5$ and $\pi = \{5\,3\,1\,2\,4\}$, then try to decrypt, 'thi w cyrms-sbo iw ooth se hatatbrls s o'. Find what the original message is. [6]

4. Write an essay of approximately 25 lines on either one of the following topics: group, polynomial, Hamming, linear, or cyclic codes, MDS, Goppa, Hadamard, or quadratic residue code, automorphism group of a code, entropy and mutual information, or cryptography. [10]